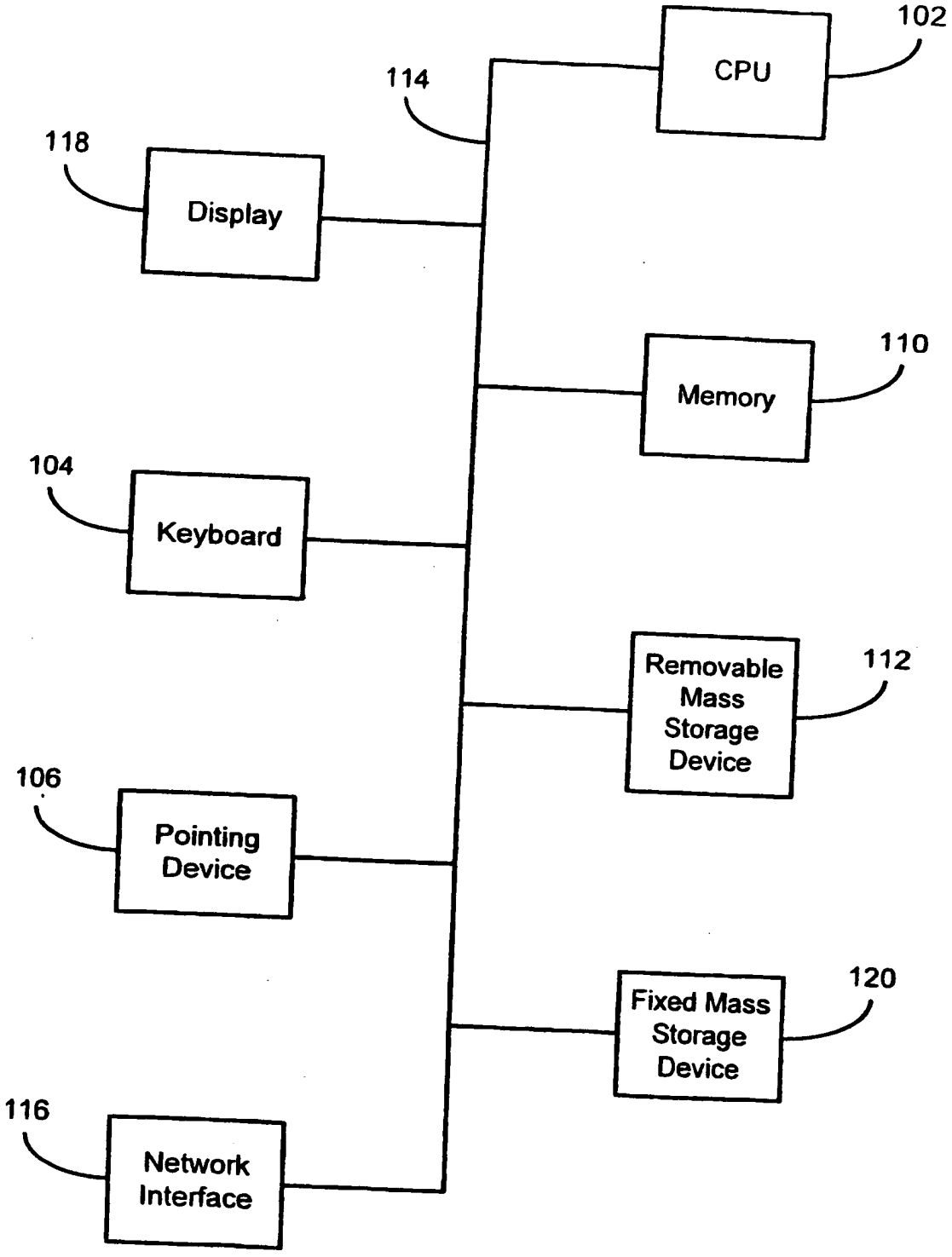

CPU
102
114
118
Display
Memory
110
104
Keyboard
Removable
Mass
Storage
Device
112
106
Pointing
Device
Fixed Mass
Storage
Device
120
116
Network
Interface

FIG 1

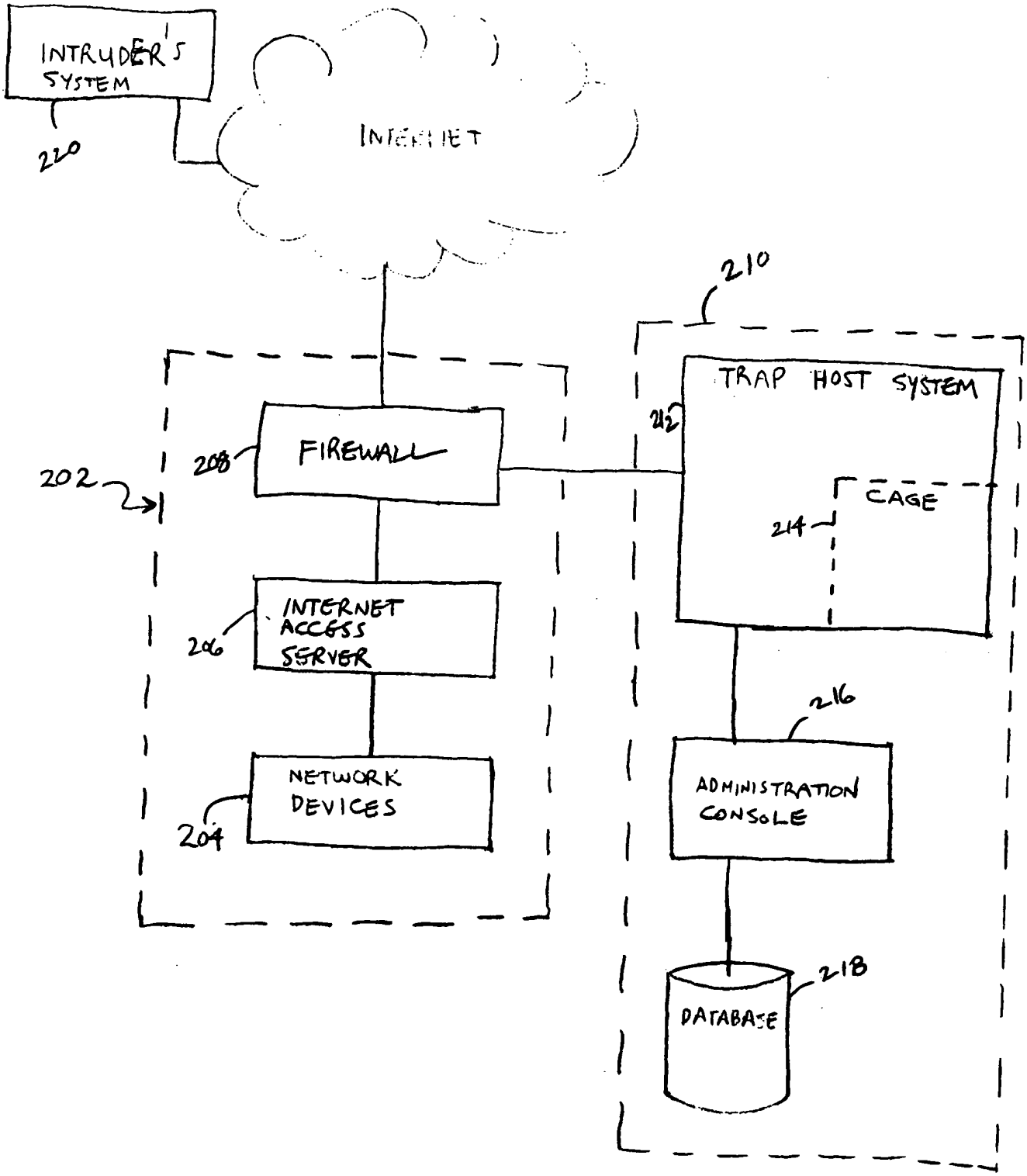

INTRUDER'S SYSTEM
220
INTERNET
210
TRAP HOST SYSTEM
212
CAGE
214
202
208
FIREWALL
INTERNET ACCESS SERVER
206
NETWORK DEVICES
204
216
ADMINISTRATION CONSOLE
218
DATABASE

FIG. 2

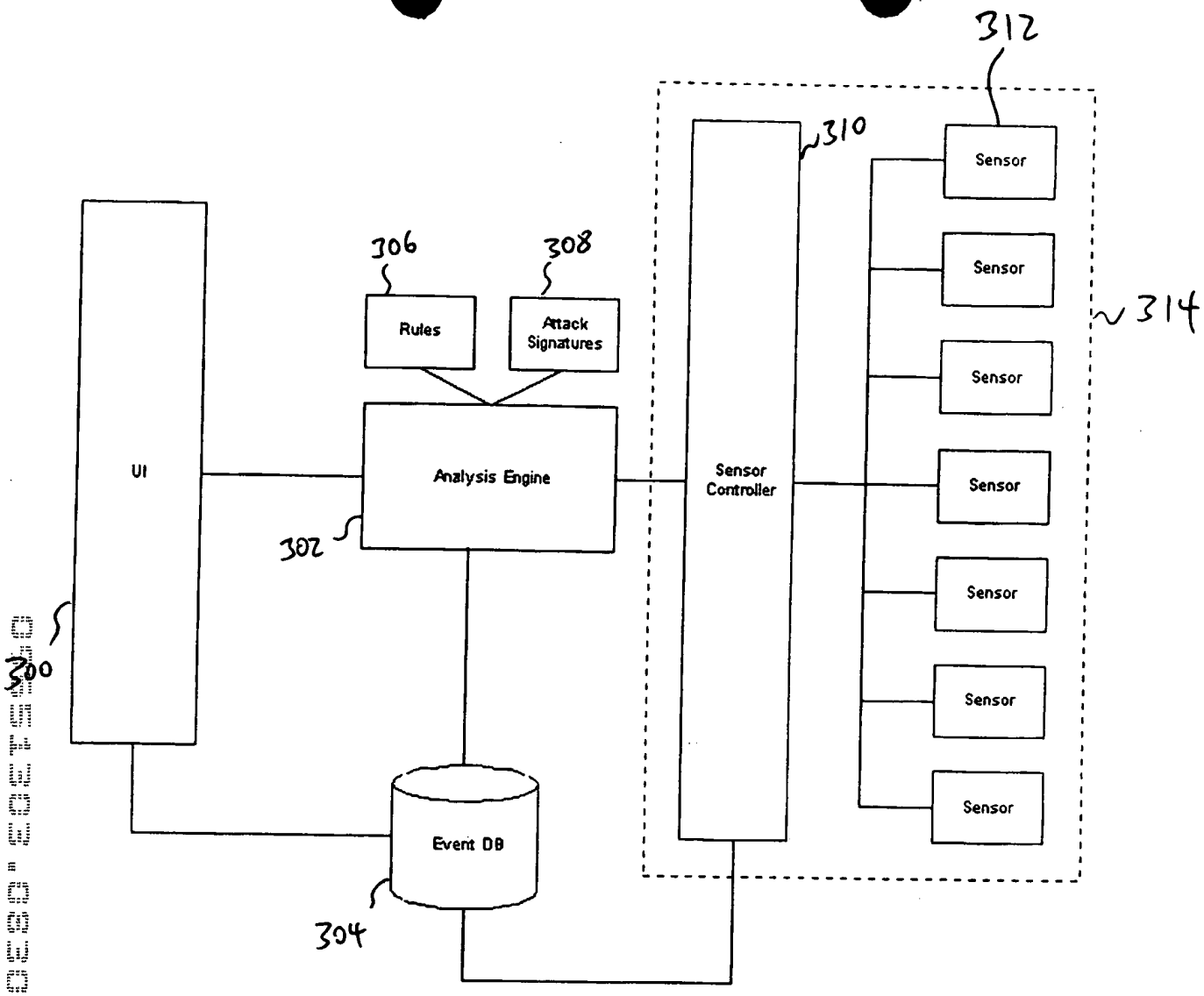

312
310
Sensor
Sensor
Sensor
Sensor
Sensor
Sensor
Sensor
314
306
308
Rules
Attack Signatures
UI
Analysis Engine
Sensor Controller
302
300
Event DB
304

FIG. 3

Pattern of Remote Break–in

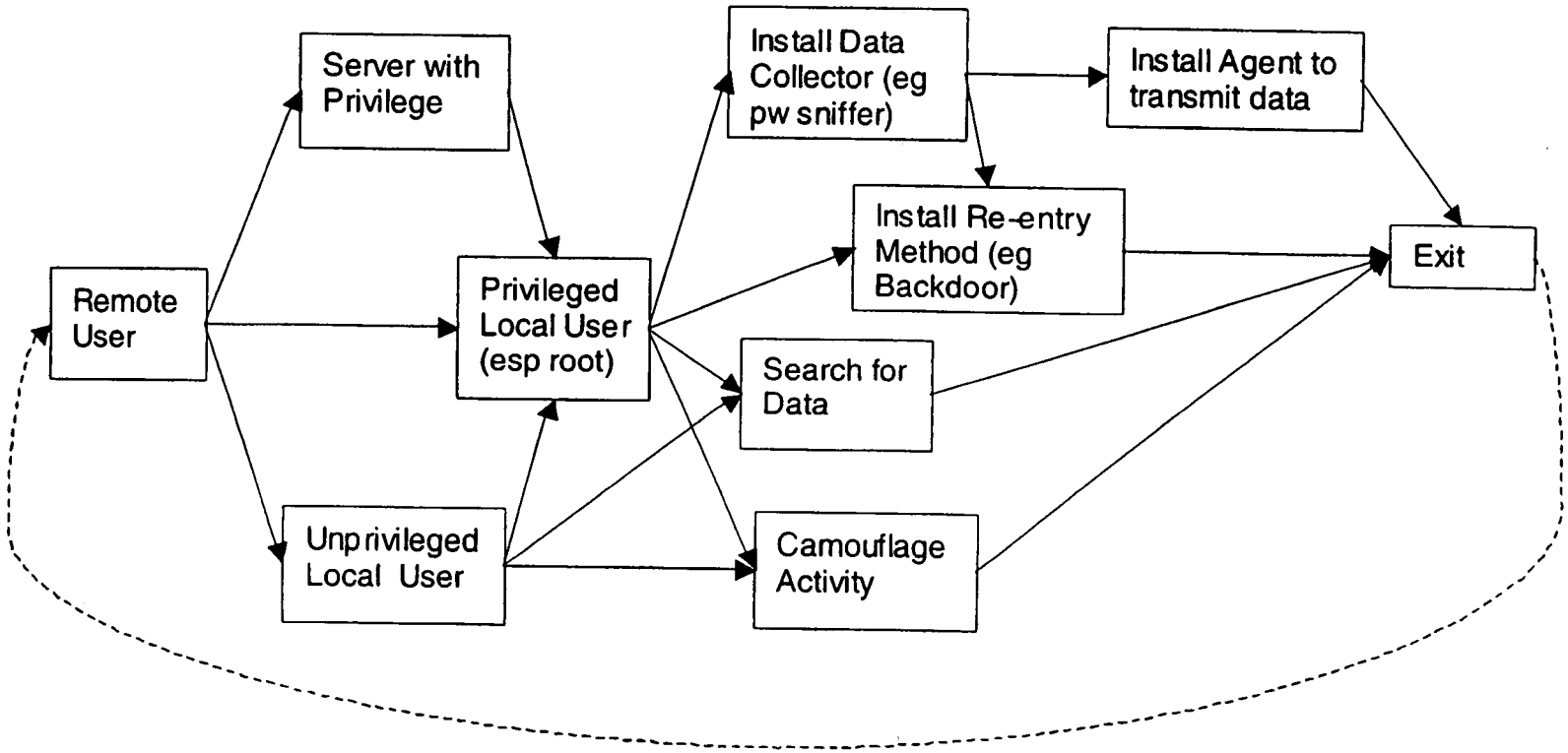


Fig 4

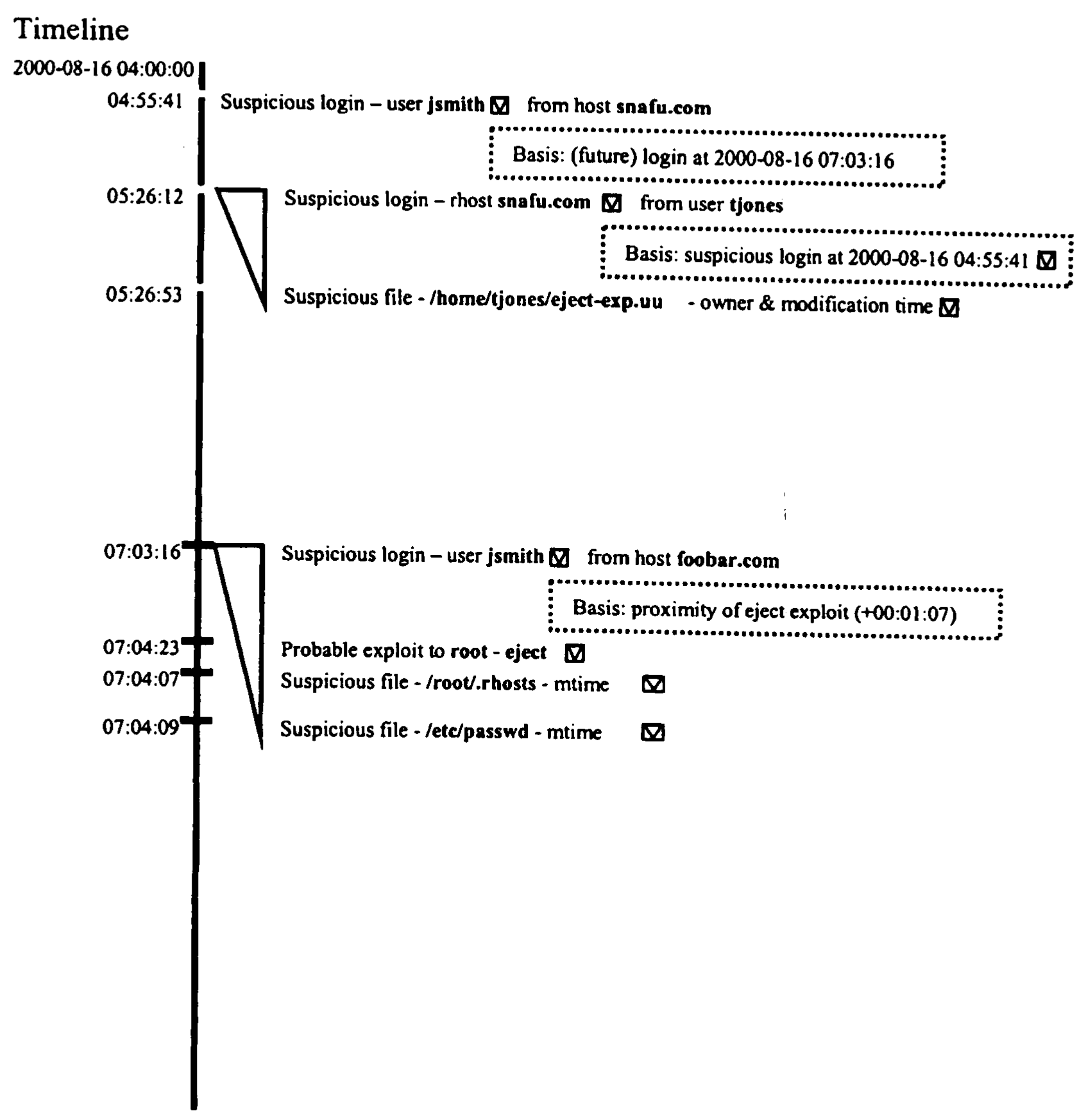
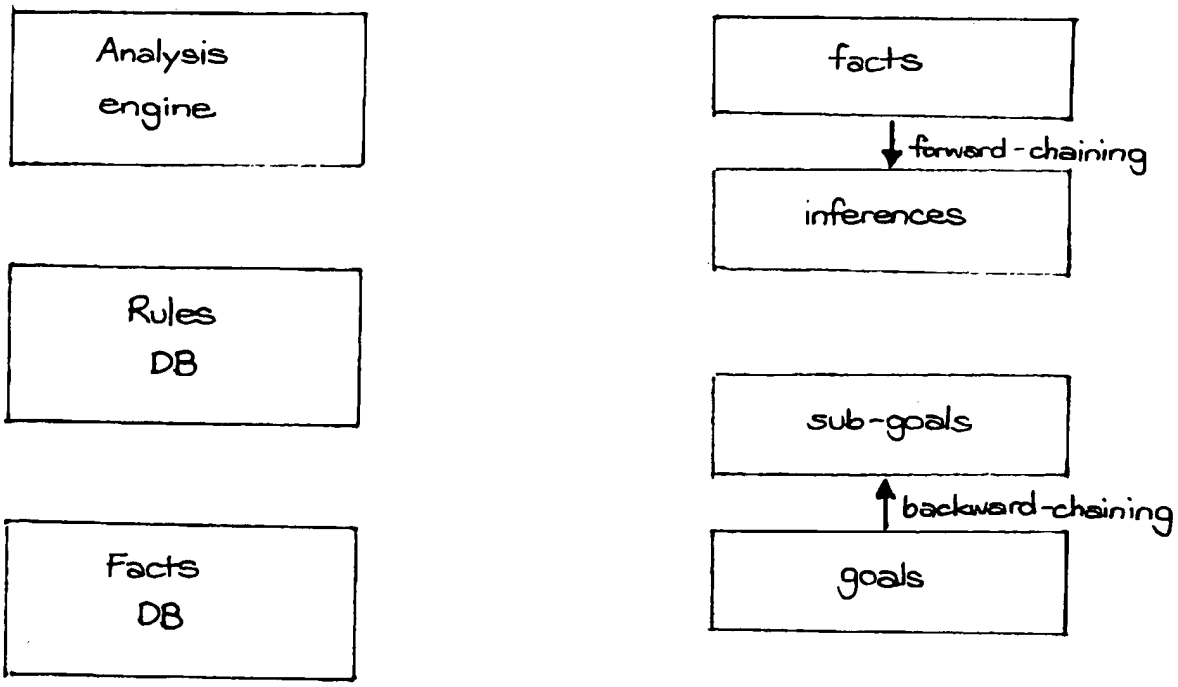

Timeline
2000-08-16 04:00:00
04:55:41
Suspicious login – user jsmith ☑ from host snafu.com
Basis: (future) login at 2000-08-16 07:03:16
05:26:12
Suspicious login – rhost snafu.com ☑ from user tjones
Basis: suspicious login at 2000-08-16 04:55:41 ☑
05:26:53
Suspicious file - /home/tjones/eject-exp.uu - owner & modification time ☑
07:03:16
Suspicious login – user jsmith ☑ from host foobar.com
Basis: proximity of eject exploit (+00:01:07)
07:04:23
Probable exploit to root - eject ☑
07:04:07
Suspicious file - /root/.rhosts - mtime ☑
07:04:09
Suspicious file - /etc/passwd - mtime ☑

FIG. 5


Analysis engine
Rules DB
Facts DB
facts
forward-chaining
inferences
sub-goals
backward-chaining
goals

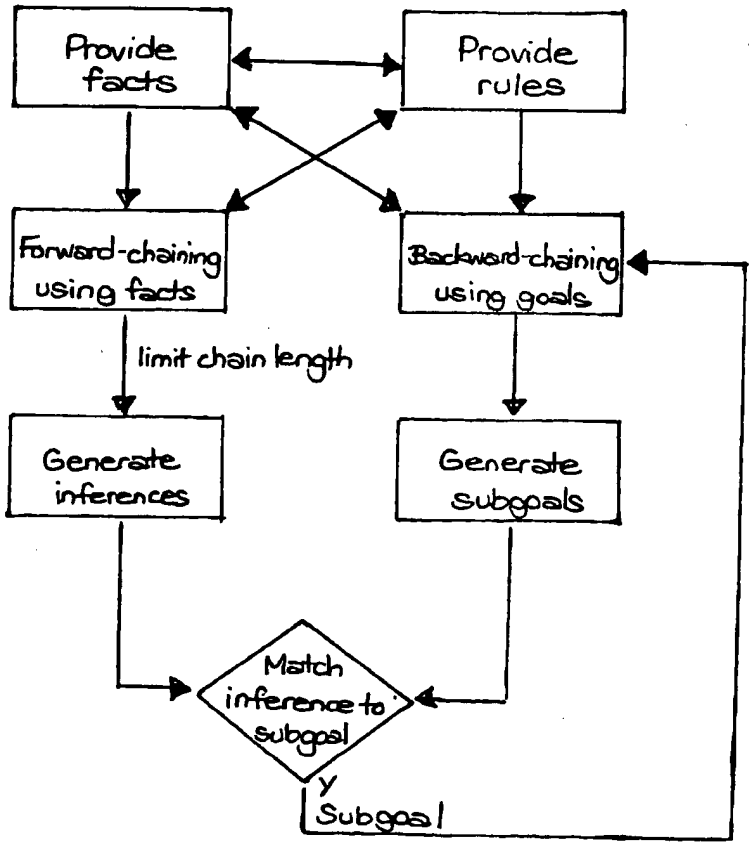

Provide facts
Provide rules
Forward-chaining using facts
Backward-chaining using goals
limit chain length
Generate inferences
Generate subgoals
Match inference to subgoal
Y
Subgoal

FIG. 6

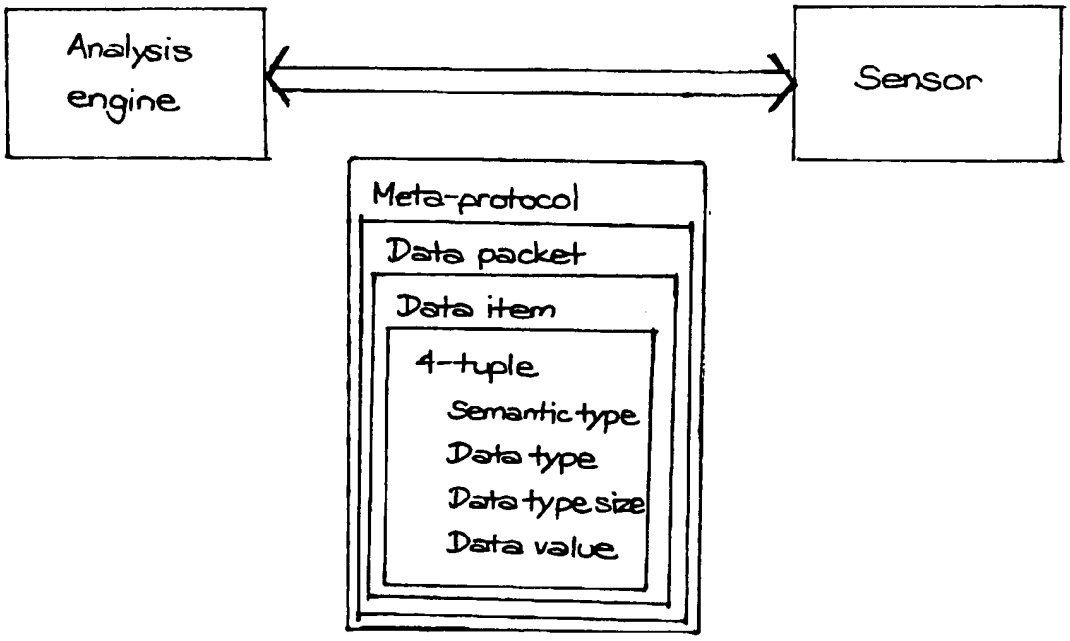

Analysis engine
Sensor
Meta-protocol
Data packet
Data item
4-tuple
Semantic type
Data type
Data type size
Data value

FIG. 7

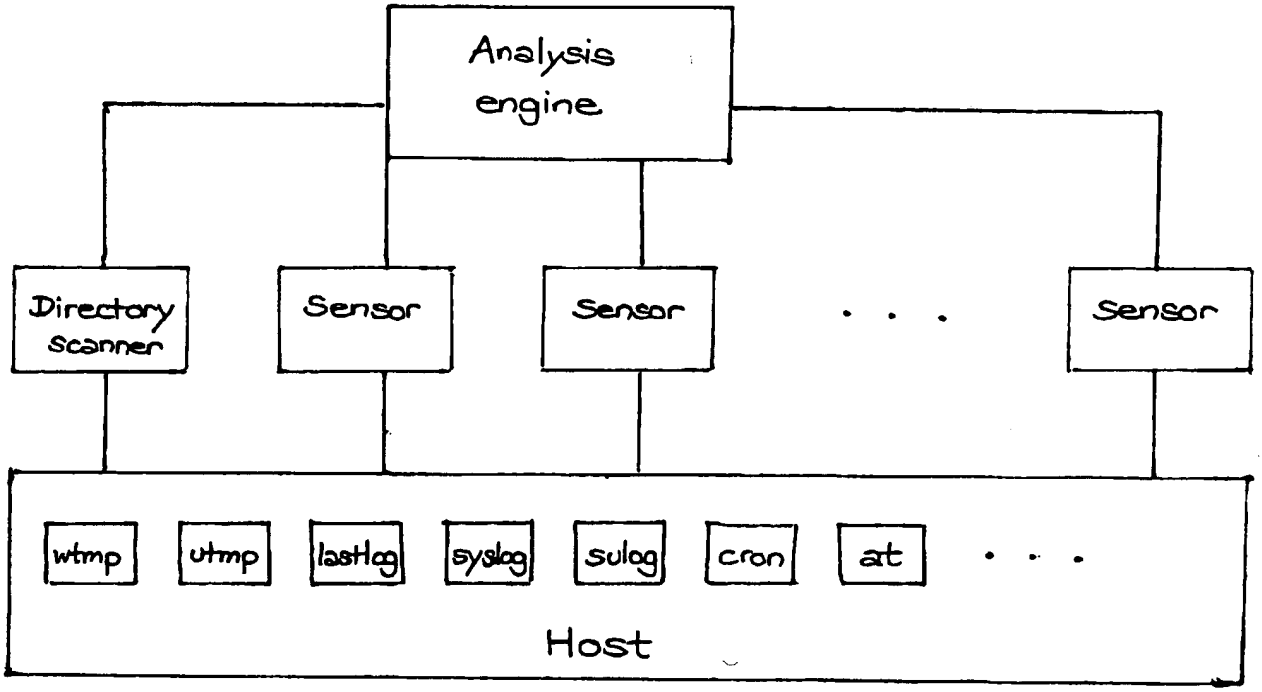

Analysis engine
Directory Scanner
Sensor
Sensor
Sensor
wtmp
utmp
lastlog
syslog
sulog
cron
at
Host

FIG. 8

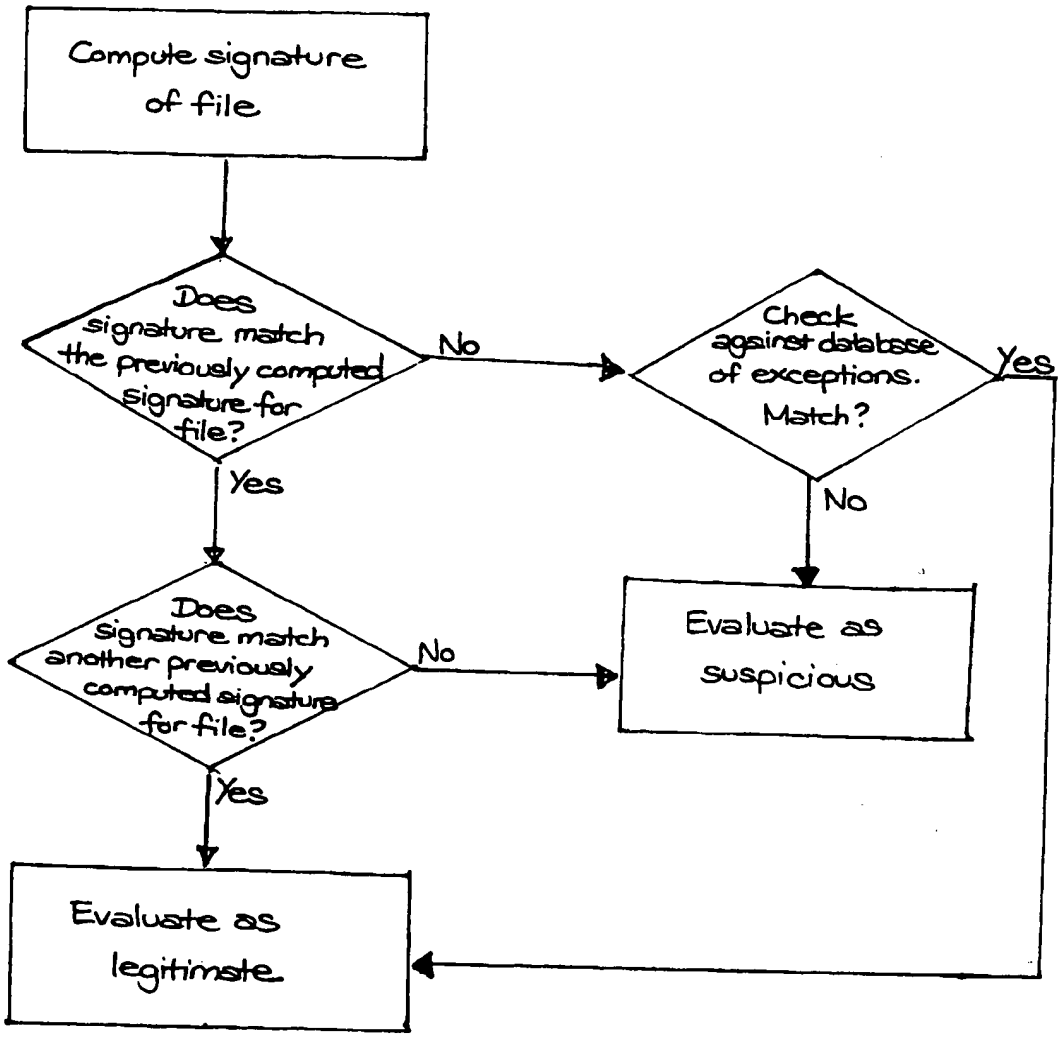

Compute signature of file
Does signature match the previously computed signature for file?
No
Yes
Check against database of exceptions. Match?
Yes
No
Does signature match another previously computed signature for file?
No
Yes
Evaluate as suspicious
Evaluate as legitimate

FIG. 9

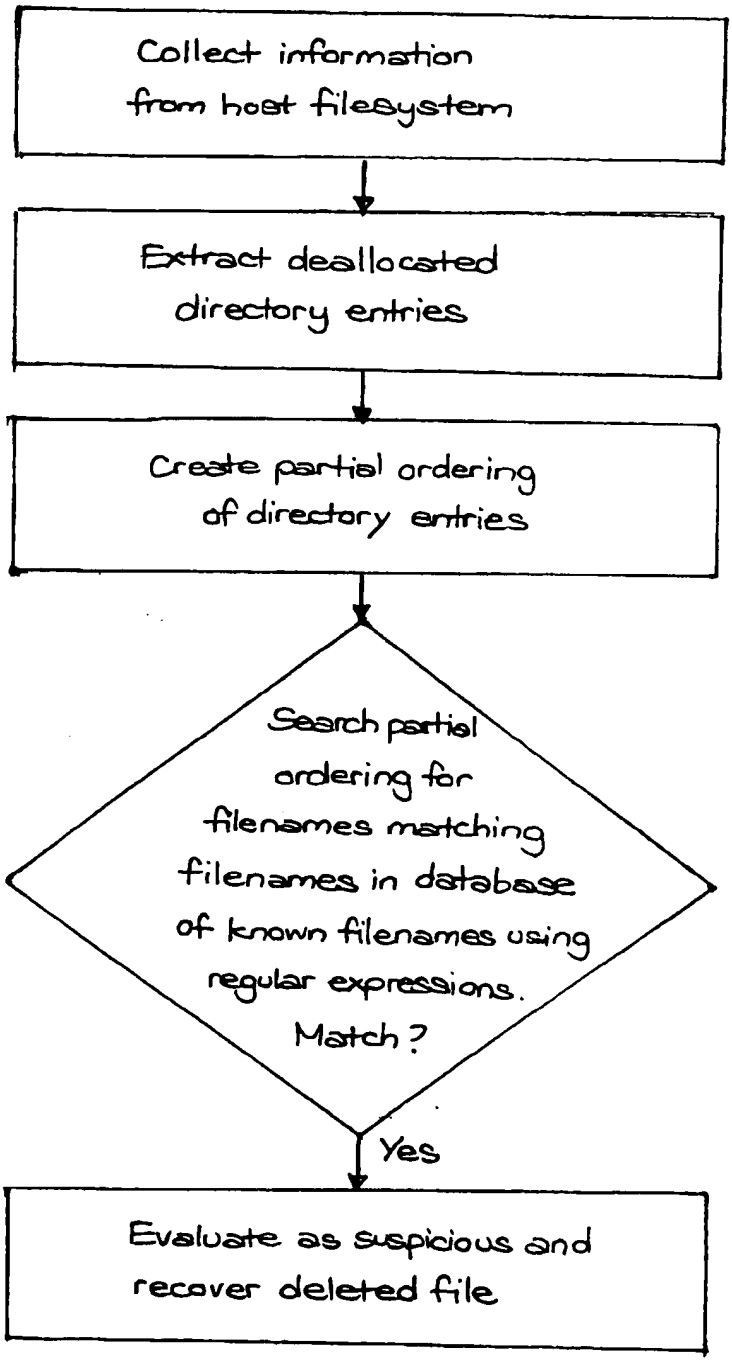

Collect information from host filesystem
Extract deallocated directory entries
Create partial ordering of directory entries
Search partial ordering for filenames matching filenames in database of known filenames using regular expressions. Match?
Yes
Evaluate as suspicious and recover deleted file

FIG. 10

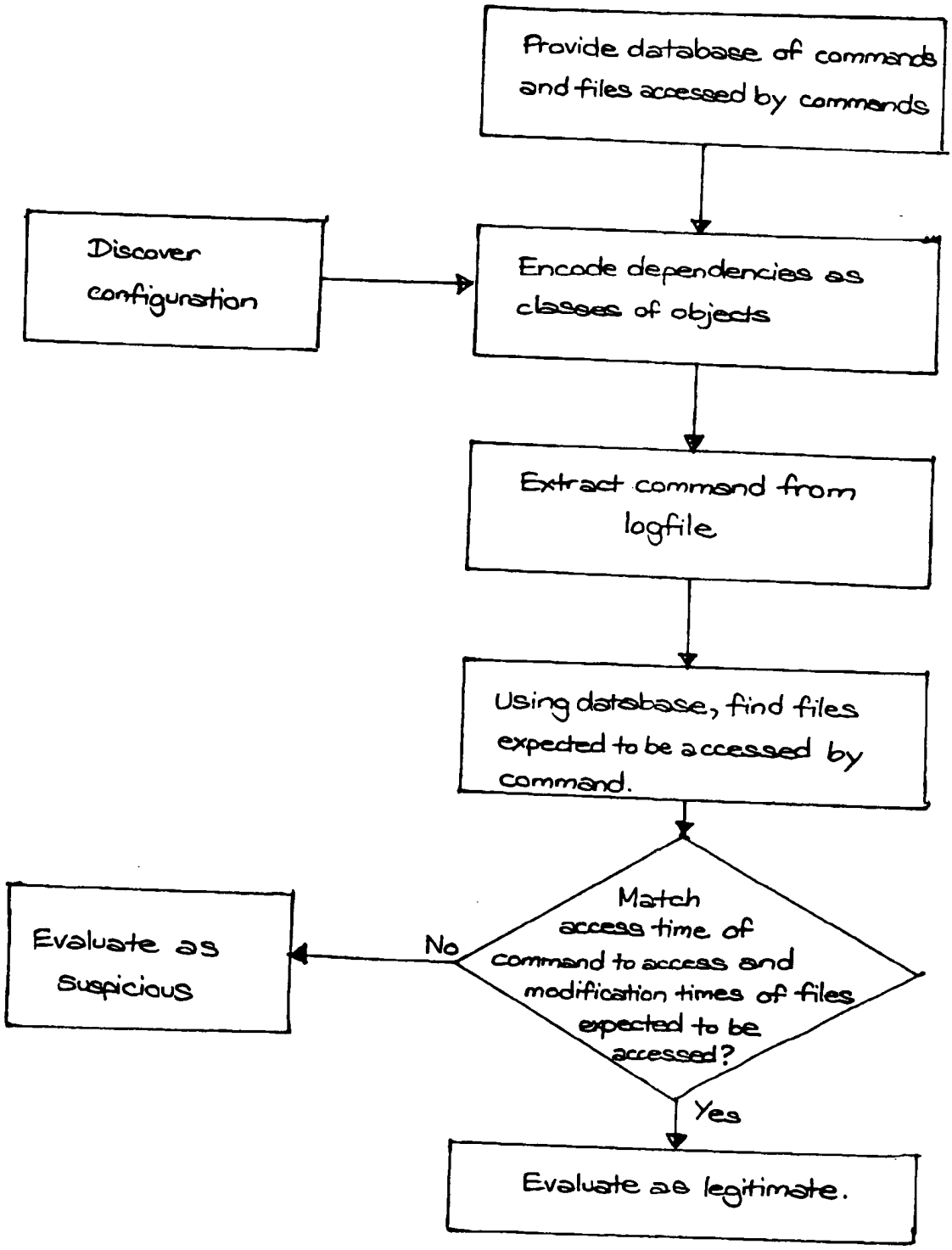

Provide database of commands and files accessed by commands
Discover configuration
Encode dependencies as classes of objects
Extract command from logfile
Using database, find files expected to be accessed by command.
Match access time of command to access and modification times of files expected to be accessed?
No
Evaluate as Suspicious
Yes
Evaluate as legitimate.

FIG. 11

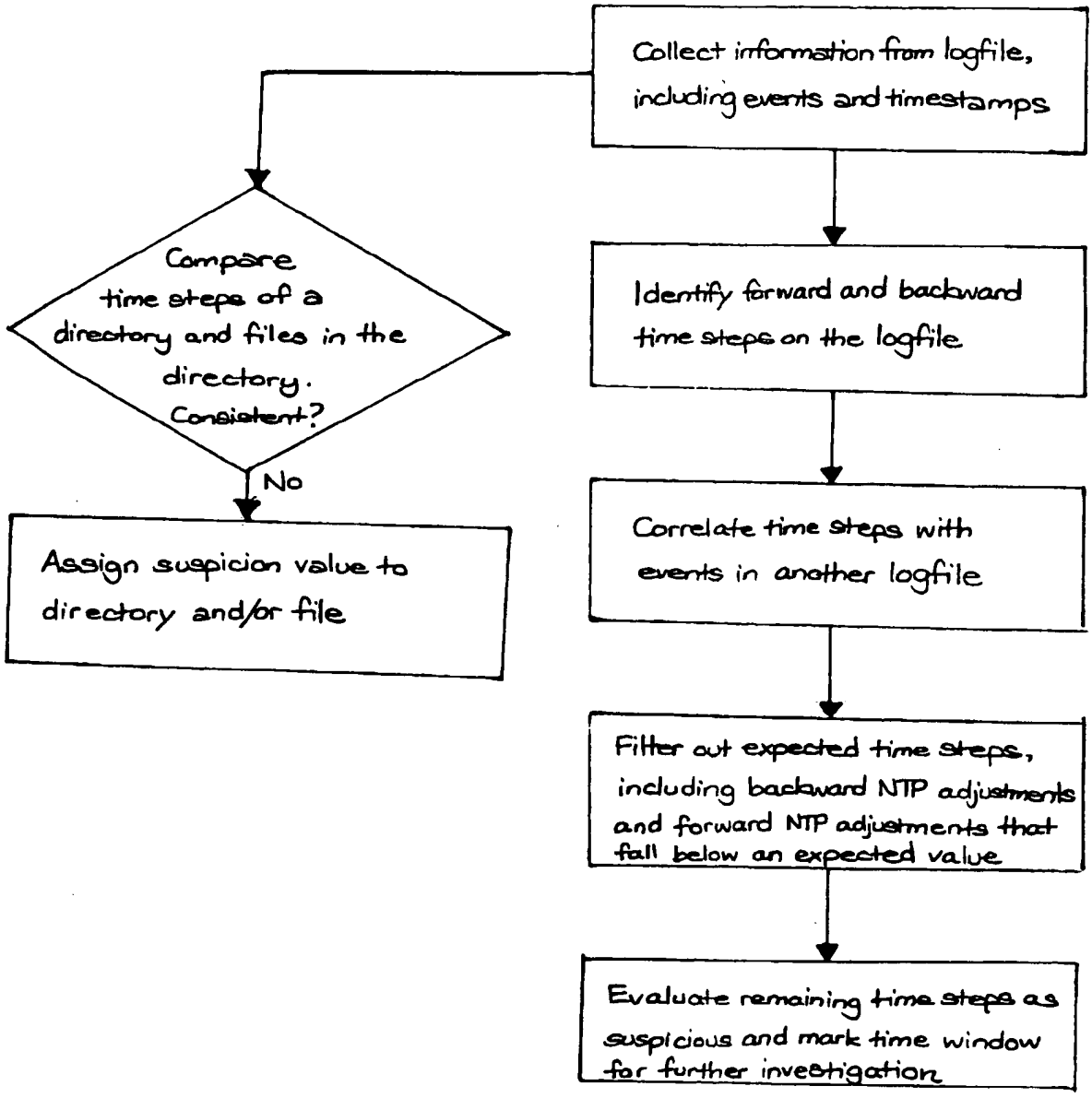

Collect information from logfile, including events and timestamps
Identify forward and backward time steps on the logfile
Correlate time steps with events in another logfile
Filter out expected time steps, including backward NTP adjustments and forward NTP adjustments that fall below an expected value
Evaluate remaining time steps as suspicious and mark time window for further investigation
Compare time steps of a directory and files in the directory. Consistent?
No
Assign suspicion value to directory and/or file

FIG. 12